

Abstract of the Disclosure

An encryption device eliminates data contention and minimizes area by accessing twice data for a given time by using a memory device of two times faster access time. The encryption device for performing encryption of plain text blocks using data encryption standard algorithm, wherein the encryption device includes an initial permutation unit, a data encryption unit having n -stage (n is an even number) pipeline structure using a first clock, a second clock and a third clock, and an inverse initial permutation unit, the encryption device includes: a multiplexer for selecting one of $n/3$ 48-bit inputs; 8 S-Boxes, each for receiving 6-bit address among the selected 48-bit and outputting 4-bit data; a demultiplexer for distributing 32-bit data from the S-Boxes to $n/3$ outputs; and a controller for control the multiplexer and the demultiplexer with a fourth clock and a fifth clock, wherein the fourth and the fifth clock are faster than the first, the second and the third clocks by $n/3$ times.